Shreetron India Limited

Revision History

Version	Issue Date	Prepared By	Approved By	Changes
1.0	02.04.2021	Vaneet Soni	A P Panwar	Initial Draft

1. Scope:

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the AUA domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

2. Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of the passwords.

Shreetron India Limited

3. Password Policy

a) The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login.
b) All user passwords (including administrator passwords) shall remain confidential and shall not be shared, posted or otherwise divulged in any manner.
c) If the passwords are being stored in the database or any other form, they should be stored in an encrypted / hashed form.
d) Password shall be changed whenever there is any indication of possible system or password compromise.
e) Complex passwords shall be selected with a minimum length of 8 characters, which:
    1. are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
    2. is free of consecutive identical characters or all-numeric or all-alphabetical groups;
    3. contains at least one numeric, one uppercase letter, one lowercase letter and one special character;
    4. shall be changed for every 3 months;
    5. shall not allow the username and password to be the same for a particular user;
    6. users shall not use the same password for various UIDAI access needs;
f) Passwords shall not be hard-coded in codes, login scripts, any executable program or files.
g) Password should not be stored or transmitted in applications in clear text or in any reversible form.
h) Password shall not be included in any automated log-on process, e.g. stored in a macro or function key.
i) Three successive login failures shall result in user account being locked; they should not be able to login until their account is unlocked and the password reset. The user shall have to contact the System Engineers/Administrators for getting the account unlocked.

---- End of the document----